THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:	
Information associated with Apple ID mooter1017@icloud.com that is stored at premises controlled by Apple.	Case No. 5:20mj1133 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Keith Lewis, a Special Agent (S/A) of the Bureau of Alcohol, Tobacco, Firearms and Explosives, being duly sworn on oath, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. Affiant is a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), United States Department of Justice, and has been so employed since March 2014. Prior to becoming a Special Agent with ATF, the Affiant was an Officer with the United States Secret Service from December 2010 through March 2014. The Affiant has completed the

Uniformed Police Training Program, the Federal Criminal Investigator Training Program and the ATF Special Agent Basic Training at the Federal Law Enforcement Training Center in Glynco, Georgia. The Affiant has also completed the United States Secret Service Officer Basic Training Course in Beltsville, Maryland. In addition to the firearms, arson, and explosives related training received in these courses, the Affiant has also conducted and participated in numerous investigations involving firearms, firearms trafficking, and narcotics.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents and law enforcement officers; from my discussions with witnesses involved in the investigation; and from my review of records and reports relating to the investigation. Unless otherwise noted, wherever in this Affidavit I assert that a statement was made, the information was provided by another special agent, law enforcement officer or witness who had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Since this Affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, contraband, instrumentalities, and/or fruits of violations of Title 21, United States Code, §§ 846 and 841 and Title 18 United States Code, 922(g)(1), as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court [is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).]

PROBABLE CAUSE

A. December 19, 2019 – Undercover Purchase of Narcotics from Hendri HOPKINS JR.

6. On December 19, 2019, an ATF S/A, acting in an undercover capacity (UC), purchased approximately 23.7 grams gross weights of suspected heroin/fentanyl analogue from HOPKINS.

7. On the same date, the ATF UC placed a recorded telephone call to HOPKINS requesting fourteen (14) grams of heroin/fentanyl analogue. HOPKINS confirmed and instructed the ATF UC to let HOPKINS know when the ATF UC was ready to conduct the transaction.

8. Later that day, the ATF UC placed another recorded telephone call to HOPKINS. HOPKINS informed the ATF UC the price for fourteen (14) grams would be $750.00 HOPKINS directed the ATF UC to meet him at the "Walgreen's" located at 20485 Euclid Avenue, Euclid, Ohio. The ATF UC arrived at the "Walgreen's" and waited for HOPKINS to arrive. HOPKINS asked the ATF UC to meet on a "side street" near the "Walgreen's" to which the ATF UC declined.

9. HOPKINS arrived to the "Walgreen's" in a dark colored Chevrolet Equinox bearing Ohio license plate HRL7919 in the company of an unknown male. HOPKINS departed the vehicle and got into the passenger seat of the ATF UC's vehicle. The ATF UC vehicle was equipped with audio and video recording.

10. HOPKINS became irritated with the ATF UC for declining to meet on a "side street". HOPKINS stated to the ATF UC "I sell dope bro, like I know this area. Like, this spot right here? This Walgreens is a hot spot…I'm the one selling you the dope. I'm the one taking the risk."

11. HOPKINS requested some type of card from the ATF UC for HOPKINS to "scoop the dope out". The ATF UC provided HOPKINS an empty "Rolaids" pack. HOPKINS placed an empty plastic bag on a digital scale provided by the ATF UC and "scooped" the narcotics into the empty plastic bag until it reached fourteen (14) grams. HOPKINS requested $800.00 for the initial fourteen (14) grams. HOPKINS was in possession of more narcotics than the ATF UC requested, so the ATF UC requested to purchase the remaining narcotics HOPKINS had. HOPKINS provided the remaining narcotics he had, in a separate plastic bag, and requested $450.00 more for the remaining narcotics. The remaining narcotics weights approximately 9.7 grams for a total of 23.7 grams. The ATF UC provided HOPKINS with a total of $1250.00 in previously recorded government funds for the narcotics.

12. HOPKINS informed the ATF UC he did not have a firearm for the ATF UC to purchase because the firearm was at HOPKINS' "girl's" house. HOPKINS removed a firearm from his waistband to show the ATF UC and stated he was considering selling it. HOPKINS informed the ATF UC the firearm was a "Glock 19, Gen 5". HOPKINS stated the firearm cost $500.00 but declined to sell the firearm to the ATF UC.

13. HOPKINS exited the ATF UC's vehicle and returned to the vehicle he arrived in, and departed the area.

14. The narcotics purchased from HOPKINS, in its packaging, was weighed to be approximately 23.7 grams.

15. ATF S/A Janna Penfield submitted the suspected narcotics purchased from HOPKINS to the Cuyahoga County Regional Forensic Science Laboratory for testing and analysis. The results of the analysis found 14.08 grams of "pale orange compressed powder and small particles" to be Heroin, Fentanyl and Carfentanil at a coverage probability of 95.45%. The results

also found 7.35 grams of "pale orange compressed powder and small particles" to be Heroin, Fentanyl and Carfentanil at a coverage probability of 95.45%.

B. January 30, 2020 – Undercover Purchase and Arrest of Hendri HOPKINS JR.

16. On January 30, 2020, an ATF UC purchased approximately 16.3 grams of fentanyl analogue from Hendri HOPKINS JR. After the undercover purchase concluded, HOPKINS was taken into custody based on a Federal Arrest Warrant for violations of 21 U.S.C. 841(a)(1) and (b)(1)(B) issued by Magistrate Judge David Ruiz on January 27, 2020.

17. On January 29, 2020, an ATF UC placed a recorded phone call to HOPKINS at (216) 688-8760. During the conversation, HOPKINS and the ATF UC agreed to meet on the following day, January 30, 2020 in order for the ATF UC to purchase narcotics from HOPKINS.

18. On January 30, 2020, the ATF UC placed another recorded phone call to HOPKINS at (216) 688-8760. During the conversation, HOPKINS directed the ATF UC to meet HOPKINS in Euclid, Ohio near East 222nd Street. The ATF UC agreed. On the same date, the ATF UC received a series of text messages from HOPKINS at (216) 688-8760. The text message conversation was as follows:

- Hendri HOPKINS (HH): Way now?
- ATF UC: 77
- HH: How much u got?
- HH: U knw what I charge 4 half
- ATF UC: Lol enough for a ½ and that 19
- ATF UC: Why you got some extra you want to sell?
- HH: Half g or half ounce?
- ATF UC: ½ ounce
- ATF UC: I ain't no lil g guy
- ATF UC: 800?
- HH: Way
- ATF UC: Dead Man's curve
- HH: Get off on 200
- ATF UC: WYA I don't want to chase you around again
- HH: 200
- ATF UC: K

19. A short time later, the ATF UC called HOPKINS to inform HOPKINS the ATF UC was in the area. HOPKINS directed the ATF UC to meet him at the Drug Mart (725 East 200th Street, Euclid, Ohio). A short time later, HOPKINS called the ATF UC informing the ATF UC that HOPKINS had "15 grams" with him for sale. The ATF UC and HOPKINS negotiated a price of $70.00 per gram.

20. A short time later, HOPKINS called the ATF UC to inquire where the ATF UC was. The ATF UC informed HOPKINS he was parked at the O'Reilly's store (689 East 200th Street, Euclid, Ohio). HOPKINS arrived to the parking lot of the O'Reilly's store driving a blue Mazda sedan bearing Ohio license plate #HIX2001. HOPKINS exited his vehicle, and walked across the parking lot to the ATF UC's vehicle and entered the passenger seat. The ATF UC's vehicle was equipped with audio and video recording devices.

21. After some casual conversation, HOPKINS removed a bag or suspected fentanyl analogue from the front pocket of his hooded sweatshirt and placed the suspected fentanyl analogue on a digital scale provided by the ATF UC. The suspected fentanyl analogue weighed to be approximately 16.3 grams. The ATF UC provided HOPKINS $1000.00 in pre-recorded government funds for the narcotics. The ATF UC then gave an audible "bust" signal to nearby ATF arrest teams. As HOPKINS exited the ATF UC vehicle, he was taken into Federal custody.

22. During a search incident to arrest of HOPKINS' person, investigators recovered two cellular phones among other items and the pre-recorded government funds provided to HOPKINS. The two cellular phones are further described as a silver in color "Doro" cellular phone, with serial number CKC02405Z00549, and IMEI number 359574051739028 (herein after **Phone-1**) and a rose colored, "Apple iPhone" with IMEI number 357264093613470 (herein after **Phone-2**).

23. Affiant knows, based upon training and experience, that persons engaged in drug trafficking frequently utilize more than one cellular telephone at a time in an effort to evade detection by law enforcement. Affiant also knows that drug traffickers commonly switch or drop phones on a frequent basis, particularly in response to enforcement actions directed at co-conspirators. Further, Affiant knows that drug traffickers often keep records relating to their associates, including addresses, telephone and pager numbers, records relating to drug transactions and money, and that the records are often stored on the drug traffickers' cellular phone(s) and/or other electronic devices (i.e. memory devices).

24. Your affiant asked HOPKINS if he would like to provide investigators with consent to search the vehicle HOPKINS arrived in (a blue Mazda sedan bearing Ohio license plate #HIX2001). HOPKINS agreed and was provided ATF Form 3220.11 – Consent to Search, which HOPKINS stated he understood and signed. Located in the trunk of the vehicle, in a black backpack, investigators recovered forty (40) rounds of various caliber ammunition. All of the rounds of ammunition were examined by ATF SA Cory Miles and found to have been manufactured outside of the state of Ohio.

25. Your Affiant submitted the suspected narcotics purchased from HOPKINS to the Cuyahoga County Regional Forensic Science Laboratory for testing and analysis. The results of the analysis found 15.02 grams of "pink and blue small particles" to be Heroin and Carfentanil at a coverage probability of 95.45%. The results also found 0.18 grams of "eight blue and pink fragments" to be Heroin at a coverage probability of 95.45%.

26. Affiant avers that **Phone-2** has remained in evidence since their seizure, and that it has not been powered on or connected to a cellular network or the internet since January 30, 2020. In my training and experience, I know that **Phone-2** has been stored in a manner in which its

contents are, to the extent material to this investigation, in substantially the same state as they were when **Phone-2** first came into the possession of the ATF.

27. On March 20, 2020, your Affiant received a forensic examination of **Phone-1**, which is manufactured by Doro. Your Affiant received a seventeen (17)-page PDF document containing the results of the extraction. On page two (2) of the PDF document, the "username" of **Phone-1** as "12166888760" and the Mobile Station International Subscriber Directory Number (MSISDN) is identified as "12166888760". This coincides with the phone number HOPKINS was texting the ATF UC and calling from during the aforementioned undercover narcotics transaction on January 30, 2020.

28. Your Affiant knows from training and experience, narcotics traffickers, especially those who sell narcotics directly to narcotics users, often keep one phone to contact their customers, and another phone or phones to contact narcotics suppliers and maintain their personal lives. After reviewing the forensic examination of **Phone-1**, it is apparent HOPKINS used a different phone or phone(s) or other means of communication to communicate with his narcotics supplier(s) and maintain his personal life. **Phone-1**, in general, appears to have been used for the sole purpose of communicating with HOPKINS' narcotics customers.

29. On March 26, 2020, your Affiant received a forensic examination of **Phone-2**, which is an iPhone XS Max. Forensic Examiners were unable to access **Phone-2**. However, they were able to extract some device information. Examiners determined that the user of **Phone-2** entered the owner information as "IPhoneXMax" and the email address as mooter1017@icloud.com.

INFORMATION REGARDING CELLULAR PHONES

30. Affiant knows, based upon training and experience, that persons engaged in drug

trafficking require expedient forms of communication to contact suppliers, couriers, and customers; therefore, continuous access to telephone and internet communications, including cellular telephones (traditional, Smartphones, and pre-paid), and tablets (i.e. iPads), is often necessary to the success of drug traffickers. Affiant also knows that drug traffickers frequently utilize more than one cellular telephone at a time in an effort to evade detection by law enforcement. Affiant also knows that drug traffickers commonly switch or drop phones on a frequent basis, particularly in response to enforcement actions directed at co-conspirators. Further, Affiant knows that drug traffickers often keep records relating to their associates, including addresses, telephone and pager numbers, records relating to drug transactions and money, and that the records are often stored on the drug traffickers' cellular phone(s) and/or other electronic devices (i.e. memory devices).

31. Affiant knows, through training and experience, that drug traffickers often utilize cameras, cellular telephones with video/photographic capabilities, and/or video cameras and camcorders to record various aspects of their lives, to include their drug trafficking activities.

32. Affiant also knows that drug traffickers often depend upon communications to maintain their extensive contacts throughout the country and abroad. This communications system expedites the transportation of drugs from the main Source of Supply (SOS), through the drug distribution network, and eventually to the end user, the drug user. To do this, continued access to telephone and internet communication is important if not essential to maintaining timely long distance and local contacts.

33. Affiant also knows from both training and experience that telephone and internet communications are important if not essential to drug traffickers due to the distances involved in moving narcotics and coordinating the delivery of those narcotics to couriers and, ultimately,

street-level drug dealers. Affiant has personally seized numerous telephonic and internet communication devices from drug traffickers in the past. Information from these devices has provided valuable information regarding suspected criminal associates that has assisted several criminal investigations, including the phone number of the particular device, incoming and outgoing call data, dates and times of phone calls, address book information (names associated with various phone numbers), and missed, received, and dialed calls. Additionally, Affiant knows that cellular telephones and tablets commonly come equipped with digital cameras that can be used to acquire, store, transfer and transmit images and documents that can be used to facilitate the possession, use, manufacture and distribution of controlled substances. Affiant also knows that cellular phones and other electronic devices now commonly allow for the user to have internet access, which can be used in furtherance of drug trafficking activity.

34. Based upon training and experience, Affiant knows that drug traffickers utilize cellular telephones to store records, electronic receipts, notes, ledgers, contact information, customer lists, bank statements, physical addresses, and e-mail addresses, to retain and transmit photographs, text messages and e-mail messages, and to access the internet, and to communicate with other drug traffickers concerning the purchasing, transportation, sale, distribution, or possession of controlled substances.

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

35. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

36. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the

user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

37. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

38. An Apple ID takes the form of the full email address submitted by the user to create

the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

39. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

40. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided

email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

41. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

42. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data

and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

43. In my training and experience, Drug trafficking activity requires the use of secret networks in order to obtain supply of drugs to the street level from the point of origin. As previously described, communication devices are needed to carry out the necessary arrangements from street level sale to supply and/or payment for supply throughout the network, and/or communication regarding necessary arrangements to conduct drug trafficking activity. Review of the sought information may lead to information identifying sources of supply and or unknown co-conspirators. Further, review of sought information may reveal communication and/or information related to storage locations for drugs, proceeds and/or instrumentalities. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

44. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, text messages, instant messages, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

45. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

46. In my training and experience, drug trafficking communication may be conducted on text messaging apps, in a further effort to avoid detection by law enforcement. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

47. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services, in conducting drug trafficking. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users and communication made in the carrying out of drug trafficking.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

48. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment

B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant.

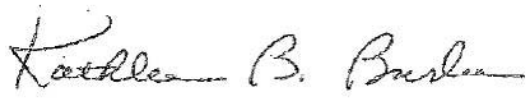
50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

51. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Keith Lewis
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

This affidavit was sworn to by the affiant by telephone after a PDF was transmitted by email, per Crim R. 41(d)(3) on this 20th day of April, 2020.



Kathleen B. Burke, U.S. Magistrate Judge